2006 Research and Development Exchange Workshop

International Collaboration on Cyber Security Research and Development:

Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response

DRAFT
Breakout Session Reports

September 22, 2006
Ottawa, Ontario, Canada

INTERIM DRAFT

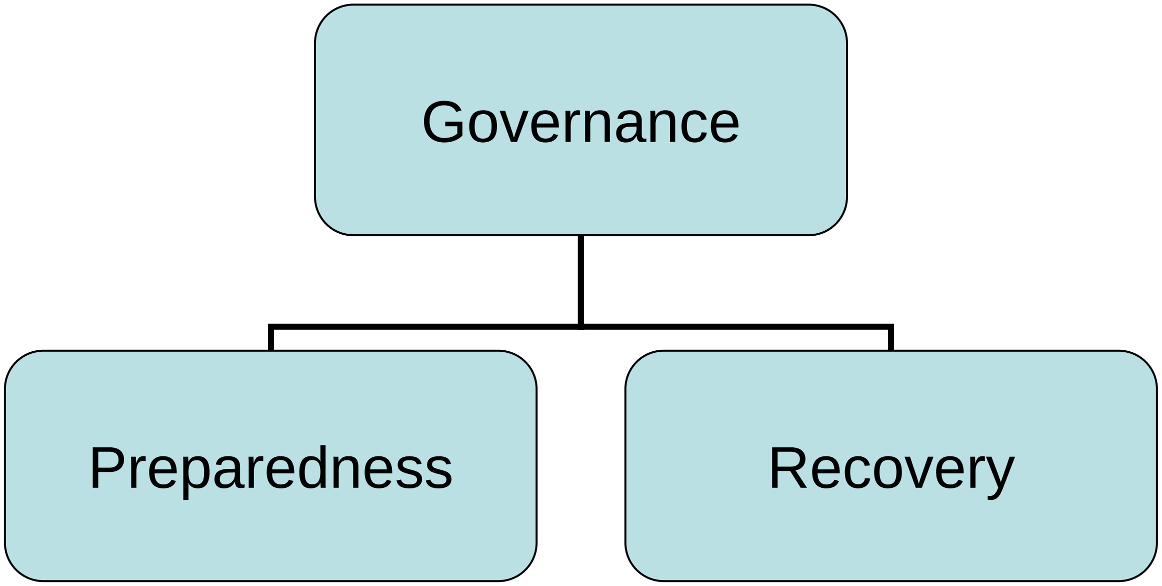
2006 RDX Workshop

International Internet Governance Breakout Session

Dr. Sy Goodman, Georgia Tech

Mr. Rod Wallace, Nortel

Governance Perspective



- Government, Nations
- Users
- Private Industry
- Technology Developers

INTERIM DRAFT

R&D Areas

Issues Subject to Governance	Components	Baseline	Governance Gap Analysis	R&D Recommendations
Infrastructure Trust	• DNS • ENUM • Secure Routing • Party and Device Authentication • Web Services	• FIPS 201 • ICANN	• Lack of Federation Standards • Legitimacy and Mandate of Current Oversight Processes	• Governance When Components Merge • 3rd Party Evaluation of Current Oversight Processes and Recommendations
Misuse and Fairness*	• SPAM (as DOS) • Mal-code that abuses infrastructure • Directed Misuse • Protocol Misuse (BOTNET) • Abuse of Web Services	• NCRCG • IDWG • NVD • CVE/OVAL • Law Enforcement	• Other Critical Infrastructure Stakeholder Involvement • Incentives, Liabilities, and Misuse of Fairness	• Common Frameworks for Information Management • Common Assessment and Mitigation Tools
Enforcement and Resolution	• Real Time Information Sharing and Coordinated During Incident Response • Information Collection About Misuse and Fairness	• IWWG • Cyber Crime Treaty	• Lack of International Enforcement Body • Lack of Common Framework • ***Multi-lateral Mechanism to Develop and Implement Criteria for Horizontal Coordination***	• Preemptive Discovery • Develop of Criteria and Process to Achieve Multi-lateral Sharing and Response

* Excludes applications level abuses such as phishing

** Input in the matrix is representative examples

Policy Issues and Agenda for Action

Policy Issues for NSTAC Consideration:

- Multi-lateralization of the national security component of network security policy while maintaining the integrity of network operations
- Maintenance of the balance in governance mechanisms between national interests (of/or articulated by Governments) and economic interests (of/or articulated by business) in operation and stewardship of critical ICT infrastructure

Agenda for Action:

1. Assessment/cataloguing of:
    - Existing rules, relationships (JCG, IWWG), analogues from other sectors (ICAO, IMO) of above
    - Baseline national governance mechanisms/policies in effect today for close allies
    - Current components that should come under governance mechanisms and evolution as we move to the NGN
2. Developing structure and membership of multi-lateral governance mechanisms to achieve the above
3. Investigate national security and economic security implications of technical and economic convergence

Global-Scale Identity Management Breakout Session

Mr. Reg Foulkes, CSC Canada

Dr. Tim Moses, Entrust

Current R&D Activities

The following R&D activities are currently underway, which address *global-scale* identity management and serve to strengthen communications and cyber security:

Some activities and initiatives have attempted to be global, but have only reached a regional level:

- NIST / FIPS 201 (US)
- ISO SC29 & ITU-T SG13/17 (International)
- CardSpace (MSFT)
- ICAO (International)
- IdenTrust (Banking/International)
- Daidalos
- Liberty Alliance Project
- Global Grid Forum

** This area deserves further attention*

Current Standards Activities

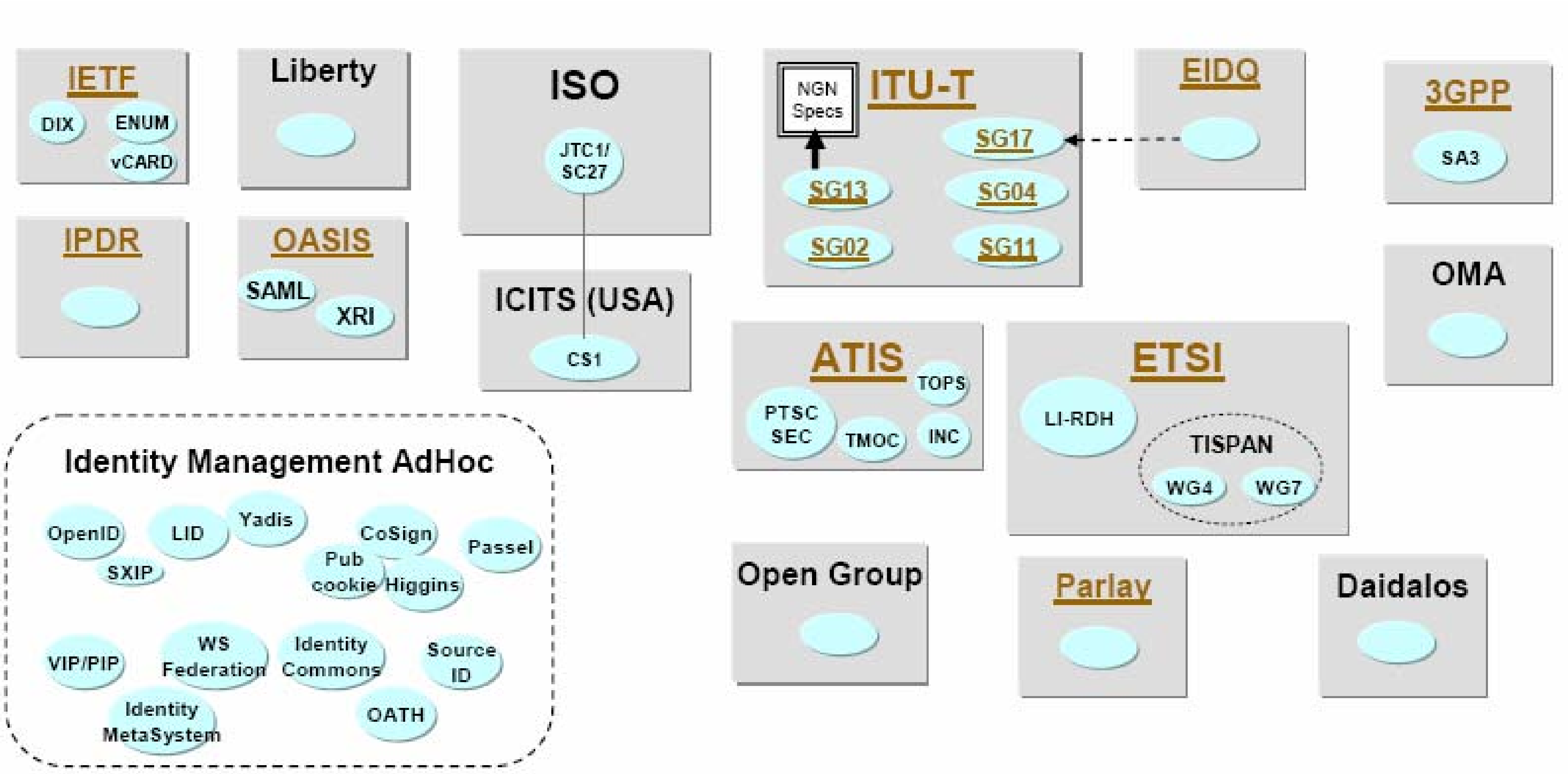


Chart excerpted from VeriSign document to ITU-T NGN Security Meeting, Oct 2006

Key Research Areas

Specific research areas offer the most potential to improve identity management R&D in the future:

- Cross-border and cross-sector use-case scenarios and requirements
  - Privacy safeguards, failure use-cases, physical v. logical, disaster recovery, contingencies
- Platform-independent credentials (wireless devices, Internet cafes, etc.)
- Interoperability amongst IDM systems
  - Framework for cross-recognition of certification practices & data schema
  - Protocols, schemas, federation models, language support, etc.
- Assurance models –reliability metrics, additional safeguards
- Trust agreements
  - Acceptable error rates
- Cost models / business cases that accelerate global-scale deployment
  - Incremental benefit
- Glossary (e.g., semantics, vocabulary, common understanding of terms)

Potential Impediments

Impediments that might inhibit the development of identity management solutions that can be scaled to a global level:

- Sovereignty issues
- Funding considerations / resource allocation (how it’s paid for)
- Infrastructure roll-out (e.g., cost, timeframe, incremental benefit)
- Diversity of platforms
- Privacy issues
- Issues of trust
- User acceptance
- Failure to agree on components of identity
- Lack of motivation to adopt global scale systems (e.g., tax breaks, regulatory mandates)

Policy Issues

Based on the session discussions, the following underlying policy issues should be studied by the NSTAC or an international counterpart:

- Ownership of identity (Fair Information Practices)
  - Transferring credentials across domains
  - Sovereignty – achieving multi-lateral agreements
- Agreed upon minimum set of attributes that constitute an identity
  - Application dependent
- Guarantees for privacy in national security and emergency preparedness applications
  - Understanding of information boundaries and privacy implications
  - Mandatory or voluntary enrolment
- Conditions for anonymity and pseudonymity including operations security
- Risk appetite (false positives and negative rates)
  - Graduated levels of assurance
- Commercial issues (trade implications, competitiveness, regulatory mandates)
- Legal and liability considerations

Roles & Responsibilities

Industry, academia, and Government all have unique roles and responsibilities in funding and advancing R&D for identity management:

Academia	- Vulnerability research - Glossary/Taxonomy development
Industry	- Technology solutions - Identity Management in the workplace
Government (Roles for agencies responsible for regulatory, justice, and infrastructure protection)	- Incentive plan for enhanced infrastructure and security - Scenario development - Interagency collaboration
Others?	- Standards bodies - Centers of Excellence

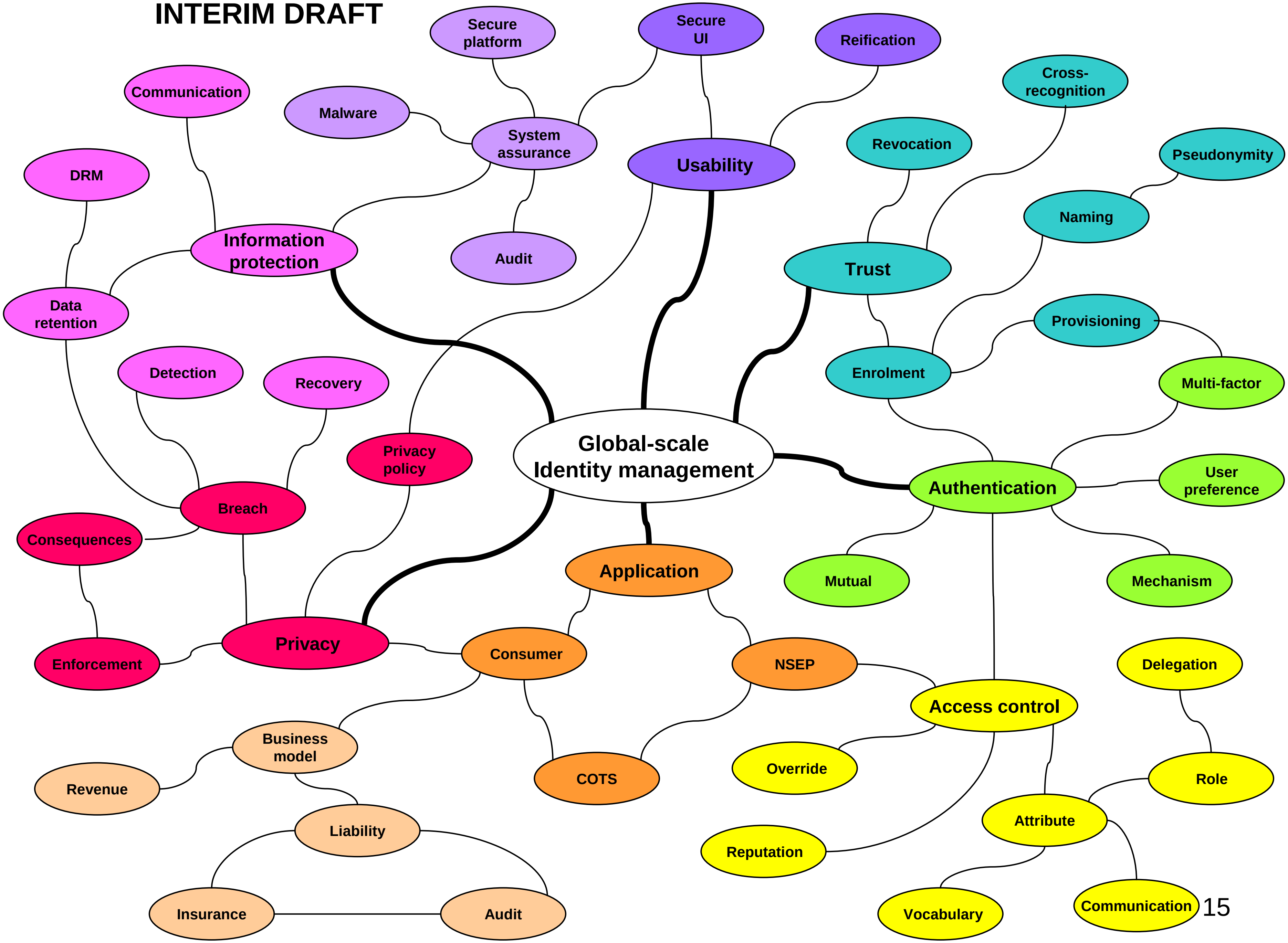
Agenda for Action

An "Agenda for Action: International Collaboration for Identity Management" should —

- Develop cross-border and cross-sector use-case scenarios and requirements
- Define ownership of identity (including transferring credentials, sovereignty)
- Identify Centers of Excellence for identity management R&D to encourage collaboration, maintain repository of ongoing initiatives, and identify promising technologies
- Agreement on models for assurance, risk and trust
- Promote education and awareness
- Glossary (e.g., semantics, vocabulary, common understanding of terms)
- Adapt policy for privacy and resolve legal and liability issues
- Advance supporting and interoperable infrastructure

Backup

INTERIM DRAFT



Global-scale Identity management

Usability
Secure UI
Reification
System assurance
Secure platform
Malware
Audit

Information protection
Communication
DRM
Data retention

Trust
Revocation
Cross-recognition
Pseudonymity
Naming
Enrolment
Provisioning

Authentication
Multi-factor
User preference
Mutual
Mechanism

Access control
Delegation
Role
Override
Attribute
Reputation
Vocabulary
Communication

Application
Consumer
NSEP
COTS

Privacy
Privacy policy
Breach
Detection
Recovery
Consequences
Enforcement

Business model
Revenue
Liability
Insurance
Audit

INTERIM DRAFT

2006 RDX Workshop

Collaborative Mechanisms for Network Security Protocol Research and Development Breakout Session

Mr. Jim Brookes, MITACS

Mr. Marc Sachs, SRI International

Goals of the R&D Consortium

Create an International R&D Consortium which:

- Enables collaboration on big ticket security research topics
  - ➢ Leverages existing funding sources to address research priorities
- Addresses the compelling network security risks to public safety issues and economic sustainability
- Identifies and works on the highest priority issues as noted by partners
- Creates a trusted collaborative environment between governments, industry, and academia

Current R&D Collaboration Mechanisms

Numerous examples of collaboration mechanisms exist for shaping future mechanisms to address cyber security concerns:

- PREDICT
- DETER
- Planet Lab
- Internet 2*
- Cylab*
- Caida
- Network Centre of Excellence
- The Technical Cooperation Panel
- European Commission Frameworks Programs*
- Public Security Technology Program
- BITS

- National Science Foundation's GENI
- Research Triangle Park
- Logic
- I3P
- Technical Support Working Group
- In-Q-tel
- SEMATECH
- IEEE
- Technology incubators
- Network Security Information Exchange

Collaborative Models

- Grant model
- Membership model
- CRADA model
- Volunteer model
- Memoranda of Understanding
- Bi and Multi-laterals
- Treaties
- Economic incentive model
- Government only
- Industry only

Strengths of Existing Collaboration Models

Several existing mechanisms possess strengths that should be considered:

- Good approach to industry involvement and funding - Cylab
- Requires involvement of multiple countries - European Commission Frameworks Programs
- Framework for future networks - Internet 2

Attributes for Collaboration

Specific attributes of a proposed collaboration model include:

- An international scope
- Support for networking and collaboration of all participants and advocacy for research
- Sustainability in the long term
- Access to real industry data by university researchers
- Safe harbor language (liability, background check laws) and relief from International Trade and Arms Regulations
- Community (government, industry, academia) endorsement
- The development of an intellectual property regime
- The provision of a funding model (supported by government and industry which provide funding and personnel; recognizes size of partner)
- The provision of a technology transition model (licensing)
- Clear guidelines for publication of results
- Trust and openness
- Meaningful output for participants

Potential Impediments

Impediments that might inhibit collaborative mechanisms for enhancing R&D:

- Intellectual property, copyright, and patent restrictions
- Export control
- Citizenship of researchers
- How to protect member data
- International Trade and Arms Regulations
- Lack of community endorsement
- Requiring clearances for students
- Ethics standards for research with humans
- Unclear equation for determining benefits based on contribution
- Commitment to sustain research
- Restrictive data markings

Why the Market Does Not Work

There is a market failure to address these compelling research issues because:

- The marketplace relies on government to address public safety, economic viability, and social issues caused by threats to the Internet and Internet technologies
- There is too much uncertainty on the risks we are facing
- Market does not effectively address public infrastructure problems
- “Magic bullet” solutions have the potential to drain important resources from longer term approaches that may be more effective in the long-term
- Scope of activity broader than any single participant
- No alignment between those who incur costs and those who benefit

Research Agenda

Top 5 priorities include:

1. Wide scale situational awareness for attack prediction and detection
2. More resilient and secure protocols
3. Global scale authentication and identity management
4. Secure and scaleable routing infrastructure
5. Security metrics

Research Agenda (continued)

Other priorities include:

1. Dynamic risk environment
2. Deployment of R&D solutions
3. Strongly authenticated network control plane
4. End user and developer appreciation for security concerns
5. Enterprise rights management
6. Assured end to end communications in a deregulated carrier environment
7. Improved and implemented software and system engineering methodologies
8. Scaleable naming system
9. Collaborative traceback of attackers
10. Support for lawful intercept
11. Authorization and policy enforcement on a wide scale
12. Information based policy enforcement (dynamic)

Policy Issues

Based on the session discussions, the following underlying policy issues should be studied by the NSTAC or an international counterpart:

- Legal concerns associated with sharing intellectual capital amongst member entities
    - ➢ Anti-trust
    - ➢ Freedom of information
- Governmental policy for sharing information across borders
- Privacy of individual citizens
- Membership eligibility criteria
- Appropriate role for governments
- Commitment to support and implement agreed upon solutions

Roles & Responsibilities

Industry, academia, and Government all have roles and responsibilities in communications and cyber security R&D collaboration:

Academia	• Provide university researchers to participate in consortium that facilitates global research • Help set research agenda • Link with other research programs
Industry	• Provide funding support • Help set research priorities • Participate in consortium that facilitates global research • Provide metrics
Government	• Provide funding support • Help set research priorities • Participate in consortium that facilitates global research • International government-to-government coordination • Link with other related-government programs • Enact appropriate laws or regulations that support collaborative research • Provide neutrality (venues/leadership)
End Users	• Help set research priorities and requirements • Provide context

Agenda for Action

The next steps to establish this international collaboration are —

- Enlist an inspiring champion to launch the initiative and:
  - Identify and communicate with key stakeholder groups
  - Define business plan
  - Develop funding proposal
  - Define and establish international collaboration framework
  - Engage international partners
- Put in place a governance model for the collaborative effort
- Develop a value proposition for each group of participants

INTERIM DRAFT

2006 RDX Workshop

Cross-Border & Cross-Sector Challenges Breakout Session

Mr. Stuart Brindley, IESO

Dr. Jack Oslund, George Washington University

Current R&D Activities

The following R&D activities are currently underway, which address cross-border and cross-sector challenges and serve to strengthen communications and cyber security:

- Existing “Roadmap to Secure Control Systems in the Energy Sector”
    - Developed by: Private Sector, DOE, NRCan, DHS, PSEPC
- The Technical Cooperation Panel (TTCP)
    - Developed by: Five allied nations
- Linking Oil Gas Industry Infrastructure Cyber Security (LOGIIC)
- Secure Wireless Communications
- DETER Testbed
- Common cyber security approach across sectors
    - Developed by: SANS Institute, DOE
    - Common Criteria

Potential Impediments

Impediments that might inhibit collaborative R&D to advance cross-sector and cross-border collaboration in the future are:

- Current collaboration is limited and localized; it should be combined and leveraged across sectors and borders
  - Initiatives are "stove-piped" or "silo-ed"; need to find common threads
  - Leadership is needed to coordinate efforts
- Secure mechanisms for information sharing across borders have not been exercised or tested
  - Need to probe deeper on interdependencies
  - Establish the "ground truth" beyond modeling efforts to date
- Sector-specific jargon exists between sectors
- Proprietary considerations can be counter-productive to information sharing
- Contrasting R&D programs between the five allied nations and European Union
- Cost and scheduling challenges in government and private sector R&D
- Managing for very low probability events

R&D Policy Issues

Based on the session discussions, the following underlying R&D policy issues should be studied by the NSTAC or an international counterpart:

- Limited willingness or ability to share classified or sensitive information intra-sector, cross-sector, and cross-border
  - Need a process for engaging people
  - “Need to share” rather than “need to know”
- Barriers to establishing new partnerships and broadening existing partnerships
  - Tendency to favor “products” over “value of partnerships”
  - Lack of information and common goals/priorities
  - Cross-sector and cross-border
- Failure to anticipate generational changes in how technology will be used
- Education – development / implementation life cycle is not in place
  - Lack of eligible potential employees for NS/EP work
- New trust structures for new online tools

Agenda for Action

An "Agenda for Action: International Collaboration for Cyber Security and Assured Communications" should —

- Create incentives for private sector to include NS/EP requirements as part of product development
- Prepare an inventory of existing R&D initiatives; identify priorities
  - Cross-sector and cross-border
  - Cyber security and information assurance
- Move beyond narrow bilaterals between governments
  - Greatly enhance private cross-sector participation
  - Build on five allied nations with common interests and goals
- Enhance R&D to probe and establish "ground truth", e.g.,
  - Interdependency modeling efforts
  - More substantive exercises
- Establish priorities for restoration and managing reduced capacity
  - "Who's on first?"

<u>An Example of Success:</u>

Leverage the "Roadmap to Secure Control Systems in the Energy Sector" and promote international collaboration

- *Adapt to telecommunications sector*
- *Broaden international collaboration*

INTERIM DRAFT

2006 RDX Workshop

Wireless and Mobile Ad Hoc Network Applications Breakout Session

Mr. Mike Alagna, Motorola

Dr. Julie Lefebvre, DRDC Ottawa

Breakout Session Members

- **Wide cross-section of participants:**
  - Industry (service providers, equipment vendors, infrastructure owners)
  - Government (U.S. and Canada)
  - Academia

- **Wide variety of perspectives:**
  - R&D Practitioners
  - Technology Implementers
  - User Community (e.g., National Security/Emergency Preparedness)

… representative of R&D Exchange participants at large

Major Discussion Themes

- Basic discussion on dimensions of issue/scope of problem – Why Mobile Ad Hoc Networks (MANET)?
  - Effective when infrastructure is lost
  - Robust connectivity (e.g., mitigate single points of failure)
  - Flexibility
  - Fault tolerance (self healing)
- Application to Emergency Response/Military/Public Safety communities:
  - Lessons Learned from Hurricane Katrina Response
  - Operability versus Interoperability
  - Scenario-specific security requirements (temporary vs. permanent app)
- Identification of Current R&D Activities/Academic Focus Areas
- Transition of current security implementations into MANET environment
- Impediments to technology adoption and further R&D
- Identification of Priorities

Current R&D Activities

The following R&D activities are currently underway, which address wireless ad hoc networks and serve to strengthen communications and cyber security:

- EU Project: WIDENS
- NIST: MANET & Sensor Network Security
- Distributed test Bed for 1st Responders
- Project Mesa
- CERDEC: Multi-Dimensional Assured, Robust Communications on-the-move Network-I (MARCOM-i) STO Program
- DARPA
- DRDC

- Strong Authentication with no central trusted authority
- Secure Routing
- Lack of Capacity
- Interoperability
- Functionality
- Intrusion Detection
- Location-based Services
- Sensors/logistics

Key Technology Areas

- Global Deployments/Registry*****
- Group Key for interoperability, dynamic changes and scale*****
- Test Bed/Standards/ Certification/Requirements*****
- Mobility/Usability*****
  - - authentication/bio metric/voice*****
  - - authorization
  - - audit
  - - QoS +Security (priority)
  - - intrusion detection/protection
  - - DOS/Protection
  - - Hybrid Nets
- 802.11 i/n automated security (and others)
- Customized simple chip/low cost
- Sensors+RFID
- Cognitive radio/SDR/Spectrum
- Privacy Issues
- Policy-based Management
- Human Factors/Interface
- Location-based service*****
- Development and Sharing of Best Practices
- IP/IPv6
- IBE
- Discovery mode strategies

**** These areas are the highest priority areas and should receive immediate attention.***

Potential Challenges & Impediments

- “No killer app in commercial space” - Lack of business case/ lack of paying “customer” for non-military use
- Lack of Vision/CONOPS for MANET deployments to justify R&D focus (e.g., separate visions addressing military and civilian space)
- Cross border coordination on ongoing R&D to leverage available R&D dollars
- Transition Issues from current environment to a secure MANET architecture
    - Human/Culture issues (in an operational environment)
    - Acceptance of multinational standards
    - Clearance level / foreign disclosure allowing info sharing
    - Lack of Forums to socialize the need
    - Export control/IPR, liability, privacy issues
    - Lack of suitable test-beds for security and accreditation
- Not enough being done: education training, standards/standardized, interoperability, bring down cost of security, testing cases involving international collaboration

Identified Priorities

- **Human Factors: Culture, Governance, Jurisdiction, Trust – in an operational environment**

Technology Investment Areas: <u>Identity Management</u> for Global, Dynamic, Technology-agnostic, Hierarchical, Meshed Networks. Technologies that meet diverse requirements of/take into account/enable communities of interest. Include culture/human factors in tech development, planning, exercises.

- **Open doors to foster collaboration, innovation, information sharing, R&D Sharing and Coordination, Standards and Policy Development**

Investment Area: applications addressing communities of interest; cost of collaboration; Inventory of current state, Increased flexibility with filtering monitoring; increased trials, info sharing forums; adequate controls (trust)

Identified Priorities (continued)

- **Hybrid networks for “Seamless Mobility”**

Investment Areas: Operability/Interoperability/Spectrum, and Assured Communications.

- Leverage military MANET R&D for commercial application
- Analyze transition/migration strategies from current security implementations to next generation MANET
- Supporting NS/EP assured communications through next generation MANET implementations, including Identity Management and Security QoS
- MANET as an enabler of “Seamless Mobility” – the killer app?
- MANET applicability to resolve spectrum management/interoperability issues?